APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/671,941	09/27/2000	Steven R. Tugenberg	GE04609	6202

22863 7590 06/10/2004	EXAMINER
MOTOROLA, INC.	BACKER, FIRMIN
CORPORATE LAW DEPARTMENT - #56-238	

	ART UNIT	PAPER NUMBER
3102 NORTH 56TH STREET PHOENIX, AZ 85018	3621	

DATE MAILED: 06/10/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

MAILED

JUN 1 0 2004

GROUP 3600

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 09/671,941
Filing Date: September 27, 2000
Appellant(s): TUGENBERG ET AL.

LAWRENCE J. CHAPA
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed April 12th, 2004.

(1)   ***Real Party in Interest***

A statement identifying the real party in interest is contained in the brief.

(2)   ***Related Appeals and Interferences***

A statement identifying the related appeals and interferences which will directly affect or

be directly affected by or have a bearing on the decision in the pending appeal is contained in the

brief.

(3)   ***Status of Claims***

The statement of the status of the claims contained in the brief is correct.

(4)   ***Status of Amendments After Final***

The appellant's statement of the status of amendments after final rejection contained in

the brief is correct.

(5)   ***Summary of Invention***

The summary of invention contained in the brief is correct.

(6)   ***Issues***

The appellant's statement of the issues in the brief is correct.

(7)   ***Grouping of Claims***

The rejection of claims 1-19 stand or fall together because appellant's brief does not

include a statement that this grouping of claims does not stand or fall together and reasons in

support thereof. See 37 CFR 1.192(c)(7).

(8)   ***Claims Appealed***

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9)   Prior Art of Record

2000/0161722   Matsushima et al   10-2002

(10)   Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2.   Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Matsushima et al

(U.S. Patent Granted Pub. 2002/0161722).

3.   As per claim 1, 12, Matsushima et al teach a method for purchasing items (*a service*

providing apparatus) over a network (*network such as the internet)* using a secure

communication device (*information processing apparatus) (see figs 1, 3, page 1 paragraph*

0008, page 3 paragraph 0050, 0059), the secure communication device including a host

processor (*recording medium, 110)*, a secure memory (*secure data area, 111)* that includes a

laser-scribed encryption key (*prestore secret key)*, and a non-secure memory (*non-secured data*

area, 112) for storing encrypted data (*encrypted personal information such credit card*) wherein

sensitive data (*personal information*) is encrypted within the secure memory using the laser-

scribed encryption key (*prestore secret key*) and stored as encrypted data in the non-secure

memory (*see page 3 paragraph, 0051, 4 paragraph 0063, 0066, 0067, 0070, 0071, 0072, 0074,*

0075), comprising retrieving an encrypted credit card number (*receive from the file serve*

encrypted personal information) and an encrypted secret key (*secret key*) from the non-secure

memory (*nonsecured memory, 112*) (*see fig 2, page 4 paragraph 0072, 0074, 0075, 0081, 0087)*

decrypting (*decrypting*) the encrypted credit card (*credit card information*) and secret key

(*media ID*) with the laser-scribed encryption key (*prestore secret key*) (*fig 5, page 5 paragraph,*

0083) encrypting (*encrypting*) the credit card number (*personal information*) with a

communication encryption key (*public key*), the communication encryption key being related to

the secret key (*see paragraph 0086*); and transferring (*transmitting*) the credit card number, as

encrypted with the communication encryption key, over the network to a destination (*file server*

130) (see fig 23, page 6 paragraph 0103, 0104).

4.   As per claim 2, Matsushima et al teach a method wherein the encrypted data is decrypted

within the secure memory using the laser-scribed encryption key and stored within the secure

memory for use by the host processor (*see page 3 paragraph, 0051, 4 paragraph 0063, 0066,*

0067, 0070, 0071, 0072, 0074, 0075) .

5.   As per claim 3, Matsushima et al teach a method further comprising receiving a personal

identification number (PIN) from a user, decrypting an encrypted PIN with the laser-scribed

encryption key, wherein transferring the encrypted credit card number is performed when the

decrypted PIN and the PIN received from the user compare (*see page 3 paragraph, 0051, 4*

paragraph 0063, 0066, 0067, 0070, 0071, 0072, 0074, 0075).

6.   As per claim 4, 13, Matsushima et al teach a method further comprising receiving

biometric information from a user; decrypting stored biometric information for the user with the

laser-scribed encryption key, performed when the decrypted biometric information compares

with the biometric information received from the user (*see page 3 paragraph, 0051, 4 paragraph*

0063, 0066, 0067, 0070, 0071, 0072, 0074, 0075).

7.   As per claim 5, Matsushima et al teach a method wherein the communication encryption

key is a common session key and wherein the method further comprises the step of generating

the session key using the secret key and information provided by the destination *(see figs 1, 3,*

page 1 paragraph 0008, page 3 paragraph 0050, 0059).

8.   As per claim 6, 14, Matsushima et al teach a method wherein the host processor and

secure memory are fabricated on an integrated circuit chip, and the encrypted data is stored in a

non-volatile memory *(see figs 1, 3).*

9.   As per claim 7, 15, Matsushima et al teach a method wherein the laser-scribed encryption

key is generated by laserscribing a semiconductor die during fabrication of the secure memory to

create a plurality of fixed "ones" and "zeroes" which make up the laser-scribed encryption key

(*see paragraph 0086*).

10.   As per claim 8, 16, Matsushima et al teach a method wherein the laser-scribed encryption

key is generated burning onetime programmable fuses on a semiconductor die during fabrication

of the secure memory to create a plurality of fixed "ones" and "zeroes" which make up the laser-

scribed encryption key (*see paragraph 0086*).

11.   As per claim 9, 17, Matsushima et al teach a method wherein the secure memory includes

blocking gates coupled between the laser-scribed encryption key and encryption logic circuitry,

the blocking gates being comprised of logic gates and have a blocking control signal input

preventing access to the laser-scribed encryption key by the encryption logic circuitry(*see fig 1

and 3*).

12.   As per claim 10, 18, Matsushima et al teach a method wherein the laser-scribed

encryption key is unique for each secure memory of a plurality of secure memories of different

processing systems (*see fig 1 and 3*).

13.   As per claim 11, 19, Matsushima et al teach a method wherein the laser-scribed

encryption key is randomly generated for each secure memory of a plurality of secure memories

of different processing systems (*see figs 1 and 3*).

(11)   ***Response to Argument***

1.   Applicant argue that the prior art, Matsushima et al '722 can not be

established as prior art based upon that the fact the reference identifies a related

application which was filed January 14, 2000 that is a continuation in part with no

indication as to what portions of the presently cited reference my have been

originally present or may have been later added. Examiner respectfully disagrees

with Applicant's argument. Examiner respectfully submits that he has reviewed the

parent case of Matsushima et al (e.g., application No. 09/482,521) filed January 14th,

2000, and found it to have support for the features relied upon by the Examiner.

However, since this case is anabandoned U.S. application that is not readily available

to the Examiner. Applicant is welcomed to independently review this application by

ordering a copy of the abandoned filed from the Office of Public Records (OPR;

Telephone number: 703-308-2733) under 37 CFR Section 1.14 (e) (1) and 37 CFR

Section 1.14 (e) (2). Applicant is notified that such a request requires payment of the

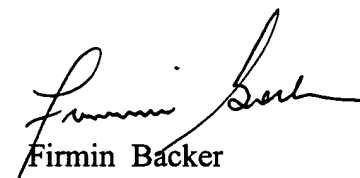fee set forth in 37 CFR 1.19 (b) (1) or 37 CFR Section 1.19(b)(2).

As such, the Examiner respectfully submits that the effective filing data of

Matsushima et al is indeed January 14th, 2000, which is older than Applicant's filing

date of September 27th, 2000.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Firmin Backer
Primary Examiner
Art Unit 3621

June 9, 2004

Conferees

John Weiss

Alexander Kalinowsky

MOTOROLA, INC.
CORPORATE LAW DEPARTMENT - #56-238
3102 NORTH 56TH STREET
PHOENIX, AZ 85018